



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/943,658	08/30/2001	Carol Lee Hobson	40655.4400	3216

7590 04/05/2007  
Thomas J. Finn  
Snell & Wilmer L.L.P.  
One Arizona Center  
400 East Van Buren  
Phoenix, AZ 85004-2202

EXAMINER
----------

HEWITT II, CALVIN L

ART UNIT	PAPER NUMBER
----------	--------------

3621

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/05/2007	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

# Office Action Summary

Application No.

09/943,658

Applicant(s)

HOBSON ET AL.

Examiner

Calvin L. Hewitt II

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 26 December 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 18-25 and 35-37 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 18-25 and 35-37 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

***Status of Claims***

1. Claims 18-25 and 35-37 have been examined.

***Response to Amendments/Arguments***

2. The Examiner recommends that the Applicant amend each of the independent claims as follows:

Remove conditional language such as if, when, may or can. And add the following language-

- [To replace the interrogating step] From a merchant website detecting the presence of a smart card reader connected to a client computer and presenting to the user a smart card payment option for using smart card as payment
- Selecting the smart card payment option by the user
- In response to the selection by the user transmitting a challenge string to the user
- In response to the challenge string, inserting a smart card into the smart card reader wherein the smart card stores a digital certificate, and entering a PIN

- Triggering by the entering of the PIN a signing of the challenge string, accessing the digital certificate and transmitting a copy of the digital certificate and the signed string to a host computer
- Authenticating by the host system the user using the signed string and the copy of the digital certificate

The rest of the claim should include the generating and utilization of a second transaction number as recited in claim 35, for example. The establishing of the channel and the "receiving" step are not necessary.

***Claim Rejections - 35 USC § 112***

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 18-25 and 35-37 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Claims 18, 23 and 35 have been amended to recite "interrogating said client computer for the presence of an authentication device". However,

Applicant's Specification is silent regarding such a process (Specification, paragraphs 12, 50 and 57).

Claims 19-24, 36 and 37 are also rejected as each depends from either claim 18, 23 or 35.

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 18-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Payne et al., U.S. Patent No. 5,715,314 in view of Purpura, U.S. Patent No. 6,421,768 and Gifford, U.S. Patent No. 5,724,424.

As per claims 18-20, Payne et al. teach an online transaction system comprising:

- receiving at a host website (payment computer) an HTTP request from a user browser (column 5, lines 25-30; column/line 9/50-10/20)

- sending said user a challenge string (column 6, lines 30-42) and authenticating said user by receiving authentication information from said user wherein the information corresponds to the user account (column 6, lines 30-59)
- generating a secondary transaction number associated with a user account and using the number to facilitate a transaction between merchant and user (column 7, lines 22-30)
- establishing an authenticated communication channel between the host and a merchant (column 7, lines 30-40)

Payne et al. disclose a host computer sending a secondary transaction number to a user and the user in turn providing the second number as payment for obtaining goods and services from the merchant (column 7, lines 15-39).

Payment "settlement" is old and well known. Therefore, it would have been obvious to one of ordinary skill for a merchant to use the payment vehicle (e.g. second transaction number) in order to collect payment (i.e. merchant submitting a payment request). Regarding the confirmation of by a merchant that a host has issued a token, Payne et al. teach a cryptographic key that is shared between host and merchant (column/line 7/65-8/2). A well-known method for securely exchanging data, such as a shared cryptographic key, is for two parties to

authenticate each other's identity using a challenge-response protocol. In one such protocol, a party A sends an encrypted (by the public key of B) random string (e.g. token) to a party B, B decrypts the string and returns the random string and a second string to A encrypted using the public key of A. A decrypts the message, verifies the first random string and if valid sends the decrypted second string back to B, thus confirming the identity of A as the original sender of the token. Payne et al. also teach communicating [claims 23-25] with a user over a distributed network (figure 1) and receiving account information from a host system to facilitate a transaction between merchant and user (column 7, lines 22-30). Payne et al. do not specifically recite a merchant redirecting a user to a host site. Purpura provides a general teaching for redirecting a user from a one computer to another over the internet (column 4, lines 46-48 and 50-55). Purpura also discloses standard techniques for establishing an "authenticated" channel between computers. For example, Purpura discloses basic key or token exchange protocols (e.g. Interlock Protocol, Challenge-response using public key decryption) where a receiving party confirms the origination of a sent token (e.g. key) (column 4, lines 7-16). More integral to Purpura's invention, however, is an authentication protocol using basic "redirection". Specifically, Purpura teaches a first computer depositing a host system signature in a user browser and a second computer decrypting the signature to authenticate the first computer or host system (column/line 3/60-4/6). However, neither Payne et al. nor Purpura

explicitly recite smart cards or payment instructions valid for only a single transaction. Gifford teaches entering a personal identification number and inserting a smart card into a smart card reader (figure 4; column/line 10/54-11/8). The Gifford system authenticates users by receiving user authentication information such as a signed challenge string (e.g. digital certificate) (column 10, lines 30-53). Gifford also authenticates users based on data extracted from a payment instrument by said authentication device (column 8, lines 1-7 and 24-31; column 10, lines 50-67). Regarding payment instructions, Gifford teaches a merchant receiving payment instruction comprising user identifier, merchant identifier, time data, and hash (column 6, lines 18-30), from a buyer (column 7, lines 38-58) wherein the instruction is checked by the merchant and/or the payment computer to determine whether the buyer is attempting to re-use the instruction (column 7, lines 56-63). Therefore, it would have been obvious to one of ordinary skill to combine the teachings of Payne et al., Purpura and Gifford in order more securely convey private data ('314, figure 2E, items 77 and 79; column 6, lines 30-59; '424, column/line 10/54-11/8), to allow a user authenticated on a first computer (e.g. via password- '768, column 3, lines 15-36; '314, figure 7) to be securely authenticated on a second site without having the user re-authenticate her/himself ('768, column 3, lines 38-43), and to prevent a customer from re-using a payment instruction ('314, column 7, lines 31-33; '424, column 7, lines 56-63; column 8, lines 52-65).



7. Claims 35-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Payne et al., U.S. Patent No. 5,715,314 in view of Gifford, U.S. Patent No. 5,724,424.

As per claims 35-37, Payne et al. teach an online transaction system comprising:

- receiving at a host website (payment computer) an HTTP request from a user browser (column 5, lines 25-30; column/line 9/50-10/20)
- sending said user a challenge string (column 6, lines 30-42) and authenticating said user by receiving authentication information from said user wherein the information corresponds to the user account (column 6, lines 30-59)
- generating a secondary transaction number associated with a user account and using the number to facilitate a transaction between merchant and user (column 7, lines 22-30)
- establishing an authenticated communication channel between the host and a merchant (column 7, lines 30-40)

Payne et al. also teach communicating [claims 23-25] with a user over a distributed network (figure 1), recognizing the presence of an authentication device on a user's computer system (figures 1, 4, 7 and 8; column 4, lines 35-37; column 7, lines 31-39; column 8, lines 33-38) and receiving account information

from a host system to facilitate a transaction between merchant and user (column 7, lines 22-30). However, Payne et al. do not specifically recite retrieving from a merchant a signed challenge string and a digital certificate. Gifford teaches entering a personal identification number and inserting a smart card into a smart card reader (figure 4; column/line 10/54-11/8). Gifford also teaches authenticating users by receiving user authentication information such as a signed challenge string (e.g. digital certificate) (column 10, lines 30-53), settlement using account numbers (figure 4; column 8, lines 17-20; column 10, lines 9-20) and a merchant receiving a payment instruction comprising user identifier, merchant identifier, time data, and hash (column 6, lines 18-30), from a buyer (column 7, lines 38-58) wherein the instruction is checked by the merchant and/or the payment computer to determine whether the buyer is attempting to re-use the instruction (column 7, lines 56-63). Therefore, it would have been obvious to one of ordinary skill to combine the teachings of Payne et al., and Gifford in order more securely convey private data ('314, figure 2E, items 77 and 79; column 6, lines 30-59; '424, column/line 10/54-11/8) and to prevent a customer from re-using a payment instruction ('314, column 7, lines 31-33; '424, column 7, lines 56-63; column 8, lines 52-65).

### ***Conclusion***

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

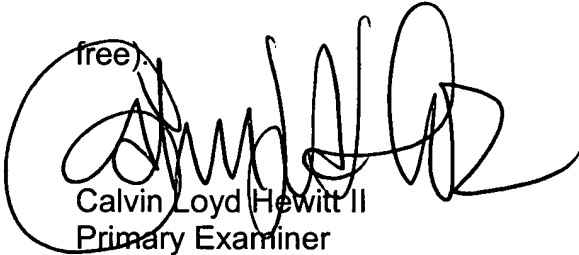
9. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Calvin Loyd Hewitt II whose telephone number is (571) 272-6709. The Examiner can normally be reached on Monday-Friday from 8:30 AM-5:00 PM.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Andrew Fischer, can be reached at (571) 272-6779.

Art Unit: 3621

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-

free).



Calvin Loyd Hewitt II  
Primary Examiner

March 27, 2007